

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-306266

(43)Date of publication of application : 02.11.2001

(51)Int.Cl.

G06F 3/06
G11B 20/10

(21)Application number : 2000-116259

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 18.04.2000

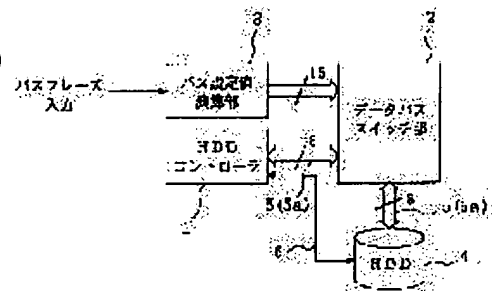
(72)Inventor : HATTA KOICHI

(54) METHOD FOR PROTECTING DATA IN HARD DISK AND COMPUTER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for protecting the data in a hard disk capable of surely preventing the leakage of data even against the situation of burglary or the like and a computer system to which this method is applied.

SOLUTION: In this method for protecting the data of an HDD 4 capable of performing data transfer through a data bus 5 with an HDD controller 1 inside a computer system, an inputted pass phrase is processed by a prescribed function, and the bit line at the HDD controller 1 side of the data bus 5 is connected to the bit line at the HDD 4 side of the data bus 5 so that a connection pattern specified by a value obtained by processing with a hash function can be obtained, and data writing is operated. When a pass phrase different from that at the time of data writing is inputted, a value different from that at the time of writing is obtained by the hash function, and the data bus 5 is turned into a connected state with a connection pattern different from that at the time of writing so that the data in the HDD 4 can be prevented from being accurately read.



木発泡の一大産地の格好のエンジニアリングシステムの削減を小ブロッカー

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2001-306266

(P2001-306266A)

(43)公開日 平成13年11月2日(2001.11.2)

(51)Int.Cl.	識別記号	F I	テ-マ-ト*(参考)
G 0 6 F 3/06	3 0 4	G 0 6 F 3/06	3 0 4 H 5 B 0 6 5
G 1 1 B 20/10		G 1 1 B 20/10	H 5 D 0 4 4

審査請求 未請求 請求項の数7 OL (全 6 頁)

(21)出願番号 特願2000-116259(P2000-116259)

(22)出願日 平成12年4月18日(2000.4.18)

(71)出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72)発明者 八田 晃一

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

(74)代理人 100061273

弁理士 佐々木 宗治 (外3名)

Fターム(参考) 5B065 BA01 CA11 CA18 PA04 PA14

5D044 AB01 BC01 CC04 DE47 HL01

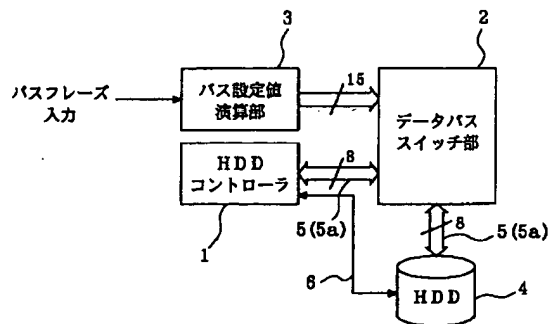
JJ06 JJ07

(54)【発明の名称】 ハードディスクのデータ保護方法及びコンピュータシステム

(57)【要約】

【課題】 盗難等の事態に対しても、データの漏洩を確実に防止することが可能なハードディスクのデータ保護方法及びこの方法を適用したコンピュータシステムを提供する。

【解決手段】 コンピュータシステム内部のHDDコントローラ1とデータバス5を介してデータ転送が行われるHDD4のデータ保護方法であって、入力されたバスフレイズを所定の関数によって処理し、ハッシュ関数による処理によって得られた値で特定される結線パターンとなるように、データバス5のHDDコントローラ1側のビット線とHDD4側のビット線とを接続してデータの書き込みを行い、データ書き込み時とは別のバスフレイズが入力された場合、ハッシュ関数によって書き込み時とは別の値が得られ、データバス5を書き込み時とは別の結線パターンの接続状態としてHDD4内のデータを正確に読み取ることができないようにする。



本発明の一実施の形態のコンピュータシステムの構成を示すブロック図

【特許請求の範囲】

【請求項1】 コンピュータシステム内部のハードディスクコントローラとデータバスを介してデータ転送が行われるハードディスクのデータ保護方法であって、入力されたパズフレーズを所定の関数によって処理し、該関数による処理によって得られた値で特定される結線パターンとなるように、前記データバスのハードディスクコントローラ側のビット線とハードディスク側のビット線を接続し、その状態でデータの書き込みを行い、データ書き込み時とは別のパズフレーズが入力された場合、前記関数によって書き込み時とは別の値が得られ、前記データバスを書き込み時とは別の結線パターンの接続状態としてハードディスク内のデータを正確に読み取ることができないようにしたことを特徴とするハードディスクのデータ保護方法。

【請求項2】 前記関数はハッシュ関数であることを特徴とする請求項1記載のハードディスクのデータ保護方法。

【請求項3】 前記関数によって得られる値は、データバスのビット幅で特定される結線パターン数を超えない、結線パターン数に最も近い2の n 乗値を構成する n ビット幅に構成されることを特徴とする請求項1又は請求項2記載のハードディスクのデータ保護方法。

【請求項4】 データバスを介してハードディスクとデータ転送を行うハードディスクコントローラを備えたコンピュータシステムであって、入力されたパズフレーズを所定の関数によって処理し、バス設定値を求めるバス設定値演算部と、ハードディスクコントローラとハードディスクとの間に設けられ、前記バス設定値演算部で求められたバス設定値を入力し、前記データバスのハードディスクコントローラ側のビット線とハードディスク側のビット線とを、前記バス設定値で特定される結線パターンとなるように接続するスイッチ部とを備え、前記ハードディスクコントローラは、パズフレーズに基づくバス設定値に従って結線されたデータバスを介してデータの書き込みを行い、前記書き込み時とは別のパズフレーズが入力された場合、前記スイッチ部によって、書き込み時のパズフレーズが入力された場合とは異なる結線パターンの接続状態とされたデータバスを介してデータを読み取ることにより、前記ハードディスクからデータを正しく読み出せないようにしたことを特徴とするコンピュータシステム。

【請求項5】 前記関数はハッシュ関数であることを特徴とする請求項4記載のコンピュータシステム。

【請求項6】 前記スイッチ部は、クロスバスイッチであることを特徴とする請求項4又は請求項5記載のコンピュータシステム。

【請求項7】 前記バス設定値は、データバスのビット幅で特定される結線パターン数を超えない、結線パター

ン数に最も近い、2の n 乗値を構成する n ビット幅に構成されることを特徴とする請求項4乃至請求項6の何れかに記載のコンピュータシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンピュータシステムにおけるハードディスクのデータ保護に関するものである。

【0002】

【従来の技術】従来、パーソナルコンピュータ（以下、PCと略す）は、電源を投入すればオペレーティングシステム（以下、OSと略す）が起動し、誰にでも使用可能な状態になるため、無断で他人に使用されてファイルをコピーされたりする危険性があった。これを防止するために、従来はOS起動前にパスワードを入力させて無断使用を防止する方法（パワーオンパスワード）が用いられていた。

【0003】

【発明が解決しようとする課題】しかしながら、このパスワードを入力する方法を採用しても、ハードディスクが装置ごと（PC本体ごと）あるいはハードディスクそのものが盗難にあった場合、ハードディスクを別の装置に接続することによりハードディスク内の機密情報などを簡単に引き出すことが可能で、情報の漏洩を防ぐことができないという問題があった。

【0004】このようなことから、盗難等の事態に対しても、データの漏洩を確実に防止することが可能なハードディスクのデータ保護方法及びこの方法を適用したコンピュータシステムの開発が望まれていた。

【0005】

【課題を解決するための手段】本発明に係るハードディスクのデータ保護方法は、コンピュータシステム内部のハードディスクコントローラとデータバスを介してデータ転送が行われるハードディスクのデータ保護方法であって、入力されたパズフレーズを所定の関数によって処理し、関数による処理によって得られた値で特定される結線パターンとなるように、データバスのハードディスクコントローラ側のビット線とハードディスク側のビット線とを接続し、その状態でデータの書き込みを行い、データ書き込み時とは別のパズフレーズが入力された場合、関数によって書き込み時とは別の値が得られ、データバスを書き込み時とは別の結線パターンの接続状態としてハードディスク内のデータを正確に読み取ることができないようにしたものである。

【0006】本発明に係るコンピュータシステムは、データバスを介してハードディスクとデータ転送を行うハードディスクコントローラを備えたコンピュータシステムであって、入力されたパズフレーズを所定の関数によって処理し、バス設定値を求めるバス設定値演算部と、ハードディスクコントローラとハードディスクとの間に

設けられ、バス設定値演算部で求められたバス設定値を入力し、データバスのハードディスクコントローラ側のビット線とハードディスク側のビット線とを、バス設定値で特定される結線パターンとなるように接続するスイッチ部とを備え、ハードディスクコントローラは、バスフレイズに基づくバス設定値に従って結線されたデータバスを介してデータの書き込みを行い、書き込み時とは別のバスフレイズが入力された場合、スイッチ部によって、書き込み時のバスフレイズが入力された場合とは異なる結線パターンの接続状態とされたデータバスを介してデータを読み取ることにより、ハードディスクからデータ

【0007】本発明においては、バスフレイズを入力させ、入力されたバスフレイズを所定の関数によって処理し、該関数による処理によって得られた値で特定される結線パターンとなるように、データバスのハードディスクコントローラ側のビット線とハードディスク側のビット線とを接続してデータの書き込みを行い、データ書き込み時とは別のバスフレイズが入力された場合、前記関数によって書き込み時とは別の値が得られ、前記データバスを書き込み時とは別の結線パターンによる接続状態にして、ハードディスク内のデータを正確に読み取ることができないようにする。

【0008】

【発明の実施の形態】図1は本発明の一実施の形態のコンピュータシステムの構成を示すブロック図である。このコンピュータシステムは、例えばPCであり、BIO Sが格納されたROM、CPU（共に図示せず）を備えたものである。更に、コンピュータシステム内にはハードディスクドライブコントローラ（以下、HDDコントローラ）1、データバススイッチ部2、バス設定値演算部3、ハードディスクドライブ（以下、HDD）4が設けられ、HDD4はデータバススイッチ部2を介してHDDコントローラ1に接続されている。5はHDD4とHDDコントローラ1とのデータ転送を行うデータバス（データ幅：8ビット）である。なお、以下では必要に応じてHDDコントローラ5側のデータバス5を5a、HDD4側のデータバス5を5cと別の符号を付して区別する。なお、ここでいうデータバス5は、単純にデータ用にのみ使用するインターフェースの場合を想定している。6は制御線で、図6に示す従来のコンピュータシステムの接続状態と同様に接続されている。なお、図6において、図1と同一部分には同一符号を付している。

【0009】データバススイッチ部2は、バス設定値演算部3から出力されるバス設定値（データ幅：15ビット）を入力する入力端子が設けられており、この入力端子に入力される値によってデータバス5aとデータバス5bの各ビット線の接続（結線）を切り替えるものである。

【0010】図2はデータバススイッチ部の構成を示す

図である。このデータバススイッチ部2は、切り替えロジック部11と結線テーブル12とクロスバススイッチ13とを備えた構成であり、結線テーブル12には、バス設定値別に構成された結線パターン指定データが格納されている。この結線パターン指定データは、クロスバススイッチ13のどの接点P_{mn}（後述する）をONにするかを指定したデータである。クロスバススイッチ13は、データバス5aとデータバス5bとの各ビット線の交差部にON/OFF自在な接点P_{mn}（m：データバス5a側の各ビットを示す0～7、n：データバス5b側の各ビットを示す0～7）が設けられ、切り替えロジック部11から出力されるデータバススイッチ信号により接点のON/OFFを行うものである。このデータバススイッチ信号の信号線は、全接点に接続されているが、図2において一部省略している。

【0011】結線パターン指定データは、クロスバススイッチ13のどの接点をONにするか（閉じるか）を指定したデータであり、切り替えロジック部11は、バス設定値演算部3からのバス設定値が入力されると、結線テーブル12を参照し、結線パターン指定データに基づくデータバススイッチ信号を駆動して指定された接点をONにし、データバス5aとデータバス5bのビット線を接続する。なお、このバス設定値は、上述したように15ビットで構成されている。以下、このバス設定値のビット幅の決定方法について簡単に説明する。

【0012】図3はバス設定値のビット数決定方法の説明図である。バス設定値は、各々8ビットで構成されたデータバス5aとデータバス5bとで考えられる結線パターン数（8！＝40320通り）を最大限に活用できるデータ幅に設定される。nビットで実現できる組合せ数は2ⁿ通りであることから、このデータ幅は、結線パターン数を超えない、結線パターン数に最も近い2のn乗値を構成するnビット幅となる。すなわち、15ビットで実現できる組合せ数は2¹⁵＝32768通り、16ビットの場合、65536通りであり結線パターン数を超えてしまい、14ビットの場合、16384通りとなり15ビットで構成した場合に比べパターン数が格段に減ってしまう。これは、言い換えればセキュリティ精度が落ちてしまうことに相当する。このようなことから、ここでは15ビット幅に構成した。

【0013】図4は、本発明の一実施の形態の動作フローチャートを示す図で、特にOSインストール時について示したものである。以下、図を参照しながら本実施の形態の動作について説明する。コンピュータシステムがパワーオンされると（S1）、CPUによってBIO Sが実行される。このBIO Sには、バスフレイズを入力させるプログラムが組み込まれており、該プログラムはバスフレイズ入力ウインドウを画面表示し、ユーザに対してバスフレイズの入力を要求する（S2）。なお、ここで「パスワード」ではなく、あえて「バスフレイズ」

という言葉を使っているが、これは、「パスワード」という言葉から受ける、例えば8文字以内とか10文字以内等の文字数制限があるかのような印象を払拭するためであり、本実施の形態のパスワードとしては、任意の長い文字数の文字列（例えば、`hirakegoma_nanamugi_namagome_namatago!`）を想定している。

【0014】ステップS2におけるパスフレーズの入力要求に従い、ユーザがパスフレーズを入力すると、バス設定値演算部3は入力されたパスフレーズをハッシュ関数で処理して15ビットのハッシュ値（バス設定値）を計算し（S3）、データバススイッチ部2に出力する。バス設定値が入力されたデータバススイッチ部2の切り替えロジック部11は、結線テーブル12を参照して前記バス設定値に対応するデータバススイッチ信号を駆動し、指定の接点をONする（S4）。ここでは、P77、P66、P55、P44、P33、P22、P11、P00の接点がONされたとする。

【0015】接点ONによってデータバス5aとデータバス5bとが接続されると、データの書き込み可能となり、ユーザはこの状態でオペレーティングシステム（以下、OSという）のインストール作業を行う（S5）。

【0016】図5はOSインストール後の起動時の動作フローチャートである。以上のようなデータバス5の接続形態の元でOSがインストールされた後に、コンピュータシステムをパワーオンした場合（S11）、上記と同様にBIOSによるパスフレーズの入力要求が行われる（S12）。ここで正確なパスフレーズが入力された場合には、OSインストール時と同様のバス設定値が得られ（S13）、これにより結線パターンもインストール時と同様となりデータを正確に読み出され、HDD4からブートアップが可能となる（S14、S15）。

【0017】これに対し、OSインストール時とは別のパスフレーズが入力された場合、バス設定値演算部3によるハッシュによってOSインストール時とは別のバス設定値が作成されることとなる（S13）。これにより例えばインストール時にONされていたP11がOFFとなつてP10がONされ、P00がOFFとなつてP01がONされたとすると（その他の接点についてはインストール時と同様の接続状態とする）、実線で示す矢印経路で書き込まれたデータが点線で示す矢印経路で読み出されることとなる。この場合、例えばデータバス5b側における正確なデータ列が例えば10101010の場合、

これをデータバススイッチ部2を介して読み出すとデータバス5a側では10101001となり、データを正しく読み出すことができない。このため、OSが起動せず（S14、S16）、HDD4内のデータを保護することが可能となる。

【0018】このように本実施の形態によれば、入力されたパスフレーズが、OSインストール時のパスフレーズと異なる場合、OSインストール時のデータバス5の結線パターンと異ならせて、データを正しく読み出すことを不能とし、OSを起動できないようにする。その結果、HDD4内のデータの漏洩を防止することが可能となり、また、汎用の機器に接続してHDD4内のデータの読み出しに対してもHDD4内のデータを保護できる。

【0019】

【発明の効果】入力されたパスフレーズが、データ書き込み時のパスフレーズと異なる場合、データ書き込み時のデータバスの結線パターンと異ならせて、データを正しく読み出すことを不能としたので、ハードディスク内のデータの漏洩を防止することが可能となり、また、汎用の機器に接続してハードディスク内のデータの読み出しに対してもハードディスク内のデータを保護できる。

【図面の簡単な説明】

【図1】本発明の一実施の形態のコンピュータシステムの構成を示すブロック図である。

【図2】データバススイッチ部の構成を示す図である。

【図3】バス設定値のビット数決定方法の説明図である。

【図4】本発明の一実施の形態の動作フローチャートを示す図である。

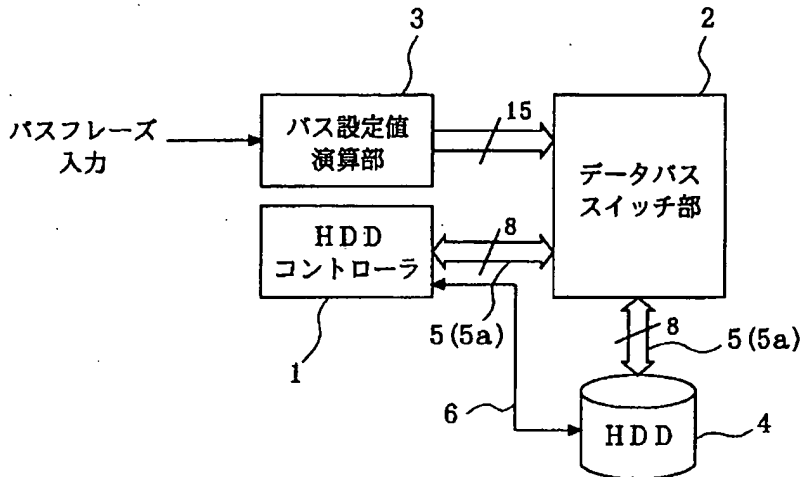
【図5】本発明のOSインストール後の起動時の動作フローチャートである。

【図6】従来の接続状態を示す図である。

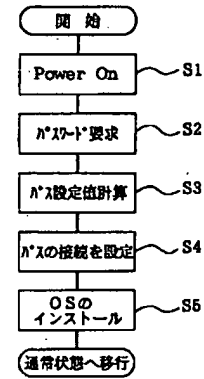
【符号の説明】

- 1 HDDコントローラ（ハードディスクコントローラ）
- 2 データバススイッチ部
- 3 バス設定値演算部
- 4 HDD（ハードディスク）
- 5 データバス
- 5a データバス（HDDコントローラ側）
- 5b データバス（HDD側）

【図1】



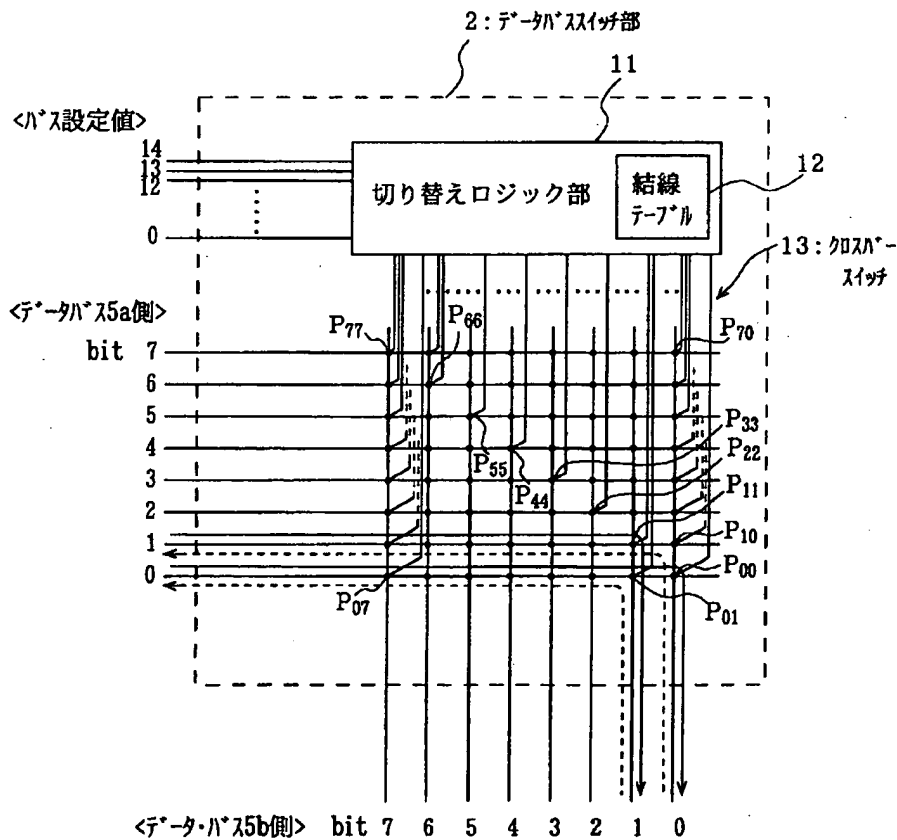
【図4】



本発明の一実施の形態の動作フローチャート

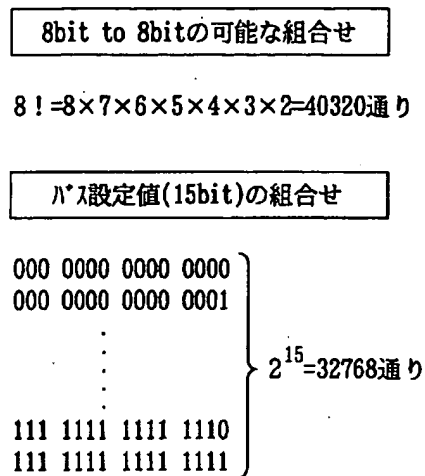
本発明の一実施の形態のコンピュータシステムの構成を示すブロック図

【図2】



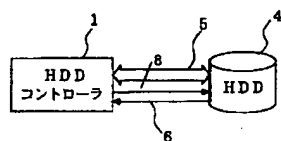
データバススイッチ部の構成を示す図

【図3】



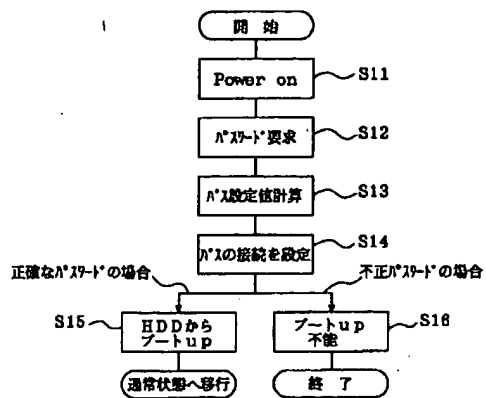
バス設定値のビット数決定方法の説明図

【図6】



従来の接続状態を示すブロック図

【図5】



OSインストール後の起動時の処理の流れを示すフローチャート